APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/490,199	01/24/2000	Michael M. Swift	202267	6863

7590 06/22/2005	EXAMINER
Leydig Voit & Mayer LTD	ORTIZ, BELIX M
Two Prudential Plaza	

ART UNIT	PAPER NUMBER
2164	

Suite 4900
180 North Stetson
Chicago, IL 60601-6780

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2005*.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications files on 16-May-2005, claims 11-12 were cancelled and

claim 1 is amended per applicant's request. Therefore, claims 1-10 are presently pending

in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at the time the invention was made to a
> person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived
> by the manner in which the invention was made.

3. Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al.

(U.S. patent No. 6,298,383) in view of Vu (U.S. patent No. 5,623,601).

As to claim 1, Gutman et al. teaches a method of enabling a proxy client in

a secured network to access a target service on behalf of a user (see column 10, lines 47-79),

comprising the steps of:

registering proxy authorization information regarding the user with a

trusted security server, the proxy authorization information identifying the proxy client and an

extent of proxy authorization, the extent of proxy authorization comprising a restriction on a

range of target services that the proxy client may access on behalf of the user (see column 1,

lines 41-45; column 1,lines 62-67; column 2 lines 1-4; and column 10, lines 51-52);

comparing, by the trusted security server, the proxy request with the proxy

authorization information of the user to determine whether to grant the proxy request (see

column 10, lines 53-55); and

issuing, by the trusted security server, a data structure containing

authentication data recognizable by the target service for authenticating the proxy client for

accessing the target service on behalf of the user (see column 1, lines 65-67 and column 9, lines

32-38).

Gutman et al. does not teach submitting, by the proxy client, a proxy request to the trusted

security server requesting access to the target service on behalf of the user.

Vu teaches method that provide a security to private and public network (see abstract), in

which he teaches submitting, by the proxy client, a proxy request to the trusted security server

requesting access to the target service on behalf of the user (see column 5, lines 16-30 and

column 8, lines 54-64).

Therefore, it would have been obvious to a person having ordinary skill in the time the

invention was made to have modifies Gutman et al. to include submitting, by the proxy client, a

proxy request to the trusted security server requesting access to the target service on behalf of the

user.

It would have been obvious to a person having ordinary skill in the time the invention was

made to have modifies Gutman et al. by the teaching of Vu, because submitting, by the proxy

client, a proxy request to the trusted security server requesting access to the target service on

behalf of the user, would enable the method of enabling a proxy client, because "The method in accordance with the invention involves protecting a private network interconnected with a potentially hostile network whereby a gateway between the two networks transparently imitates a host when a communication data packet is received from a client on one of the networks by initiating a communication session with the client. If the client is determined to have access rights to the requested service, the gateway station imitates the client to the host on the other network by initiating a communications session with the host. Thereafter, data is passed between the client session and the host session by a process which coordinates communications between the two distinct, interdependent communications sessions which proceed between the client and the gateway station and the host and the gateway station", (see Vu, column 5, lines 15-30).

As to claim 2, Gutman et al. teaches a method wherein the data structure is a ticket containing a session key for use in a session formed between the proxy client and the target service (see Gutman et al., column 2, lines 11-17).

4. Claims 3-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al. (U.S. patent No. 6,298,383) in view of Vu (U.S. patent No. 5,623,601) as applied to claims 1-2 above, and further in view of Higley et al. (U.S. patent No. 5,913,025).

As to claim 3, Gutman et al. as modified still does not teach, wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

Higley et al. teaches a method for proxy authentication to access a target

(see abstract), in which he teaches wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server (see column 2, lines 18-19).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified, to include wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified, by the teaching of Higley et al., because wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server, would enable the method to maintain the password or key in secret and the client can feel more secure using the network.

As to claim 4, Gutman et al. as modified still does not teach wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

Higley et al. teaches a method for proxy authentication (see abstract), in which he teaches wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired (see column 8, lines 16-18).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified to include wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies <u>Gutman et al.</u> as modified by the teaching of <u>Higley et al.</u>, because wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired, would enable the method to have more control of the access to the network and will be more secure for the clients.

As to claim 5, <u>Gutman et al.</u> as modified still does not teach wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

<u>Higley et al.</u> teaches a method for proxy authentication (see abstract), in which he teaches wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server (see column 5, lines 17-26).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies <u>Gutman et al.</u> as modified to include wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies <u>Gutman et al.</u> as modified by the teaching of <u>Higley et al.</u>, because wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server, would enable the method to verify the information of the authentication of the client.

As to claim 6, Gutman et al. teaches storing proxy authorization information from a user for authorizing a proxy client to act as a proxy of the user (see column 2, lines 6-10); and

determining, based on the proxy authorization information of the user, whether to grant the proxy request (see column 12, lines 20-24).

Gutman et al. does not teach a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

Higley et al. teaches authorization to access a target (see abstract), in which he teaches a computer-readable medium having computer-executable instructions (see column 4, lines 52-58 and column 5, lines 1-2) for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user (see column 5, lines 17-26).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Higley et al., because a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user, would enable the method to provide a secure network for the clients that want to use the public network.

Gutman et al. as modified still does not teach receiving a proxy request from the proxy client to access a target service on behalf of the user.

Vu teaches method that provides a security to private and public network (see abstract), in which he teaches receiving a proxy request from the proxy client to access a target service on behalf of the user (see column 5, lines 16-30 and column 8, lines 54-64).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified to include receiving a proxy request from the proxy client to access a target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified by the teaching of Vu, because receiving a proxy request from the proxy client to access a target service on behalf of the user, would enable the method of enabling a proxy client, because "The method in accordance with the invention involves protecting a private network interconnected with a potentially hostile network whereby a gateway between the two networks transparently imitates a host when a communication data packet is received from a client on one of the networks by initiating a communication session

with the client. If the client is determined to have access rights to the requested service, the

gateway station imitates the client to the host on the other network by initiating a

communications session with the host. Thereafter, data is passed between the client session and

the host session by a process which coordinates communications between the two distinct,

interdependent communications sessions which proceed between the client and the gateway

station and the host and the gateway station", (see Vu, column 5, lines 15-30).

As to claim 7, Gutman et al. as modified teaches a computer-readable medium having

further computer-executable instructions for performing the step of authenticating the user based

on a password of the user before storing the proxy authorization information (see Higley et al.,

column 5, lines 20-21).

As to claim 8, Gutman et al. as modified teaches a computer-readable medium wherein the

step of receiving the proxy request includes authenticating the proxy client based on a ticket

issued to the proxy client for communicating with the trusted security server (see Higley et al.,

column 2, lines 18-19).

As to claim 10, Gutman et al. as modified teaches a computer-readable medium wherein

the data structure is encrypted with a key shared by the target service and the trusted security

server (see Higley et al., column 2, lines 18-19).

5.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Gutman et al.</u>

(U.S. patent No. 6,298,383) in view of <u>Vu</u> (U.S. patent No. 5,623,601) and further in view of

<u>Higley et al.</u> (U.S. patent No. 5,913,025) as applied to claims 3-8 and 10 above, and still further

in view of <u>Subramaniam et al.</u> (U.S. patent No. 6,081,900).

As to claim 9, <u>Gutman et al.</u> as modified still does not teach a computer-readable medium

having further computer-executable instructions for performing the step of sending the data

structure to the proxy client for presenting to the target service for authentication of the proxy

client.

<u>Subramaniam et al.</u> teaches method and system are provided for secure access to a network

(see abstract), in which he teaches a computer-readable medium having further

computer-executable instructions for performing the step of sending the data structure to the

proxy client for presenting to the target service for authentication of the proxy client (see column

15, lines 29-38 and column 16, lines 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the time the

invention was made to have modifies <u>Gutman et al.</u> as modified to include a computer-readable

medium having further computer-executable instructions for performing the step of sending the

data structure to the proxy client for presenting to the target service for authentication of the

proxy client.

It would have been obvious to a person having ordinary skill in the time the invention was

made to have modifies <u>Gutman et al.</u> as modified by the teaching of <u>Subramaniam et al.</u>, because

wherein the security principal is a client on the secured network, would enable the method to be

sure that the client has authorization, and that made the network more secure.

Response to Arguments

6. Applicant's arguments filed 16- May- 2005 with respect to the rejected claims in view

of the cited references have been fully considered but they are not found persuasive:

In response to applicants' arguments that "Gutman et al, fail to teach or suggest

registering proxy authorization information regarding the user with a trusted security server, the

proxy authorization information identifying the proxy client and an extent of proxy

authorization, the extent of proxy authorization comprising a restriction on a range of target

services that the proxy client may access on behalf of the user", the arguments have been fully

considered but are not deemed persuasive, because Gutman et al. teaches "Traditional

wholesale ISPs and Roaming Service Providers offer network access through a technique called

Authentication proxying" (see Gutman et al., column 1, lines 41-43).

"Hence, the ISP will "proxy" out the authentication transaction to the corporation. An

AAA service within the corporation then identifies the user, verifies the password, and

provisions the user. Then the AAA service notifies the ISP's proxy server that the user is

acceptable and passes along provisioning details associated with the user (such as an IP address

to use or a pool identification of an IP address pool from which an IP address needs to be

allocated). The ISP then grants the user access to the network based upon the reply it gets back

from the corporation", (see Gutman et al., column 1,lines 62-67; column 2 lines 1-4).

In response to applicants' arguments that "Gutman et al, fail to teach or suggest

proxy authorization information", the arguments have been fully considered but are not deemed

persuasive, because Gutman et al. teaches "What really happens in that scenario is that the ISP

determines that the user belongs to Corporation A (Corp.sub.A) by parsing either the fully

qualified domain name (FQDN) supplied by the user, a DNIS ID, or some other mechanism.

Having determined that the user trying to gain access belongs to Corp.sub.A, the ISP cannot

really authenticate the user. As noted earlier, the user's record is still with the corporation.

Hence, the ISP will "proxy" out the authentication transaction to the corporation. An AAA

service within the corporation then identifies the user, verifies the password, and provisions the

user. Then the AAA service notifies the ISP's proxy server that the user is acceptable and

passes along provisioning details associated with the user (such

as an IP address to use or a pool identification of an IP address pool from which an IP address

needs to be allocated). The ISP then grants the user access to the network based upon the reply

it gets back from the corporation. This technique is called proxying", (see Gutman et al.,

column 1, lines 55-67 and column 2, lines 1-5).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Belix M. Ortiz whose telephone number is 571-272-4081.

The examiner can normally be reached on moday-friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Dov Popovici can be reached on 571-272-4083. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

bmo

June 15, 2005

SAM RIMELL
MARY EXAMINER